

## CLAIMS

What is claimed is:

1           1.       A method for providing a hash and a complement of the hash for an item in a  
2 computer system, the method comprising the steps of:

3           (a)     providing a plurality of components from the item, the plurality of  
4 components including a first component and a last component, each of the plurality of  
5 components includes a particular number of bits;

6           (b)     cascading the plurality of components through at least one XOR to provide a  
7 plurality of resultants, the plurality of resultants including a first resultant and a final  
8 resultant, the final resultant including only the last component and the first resultant  
9 including an XOR of the first component and remaining cascaded components of the  
10 plurality of components;

11          (c)     applying an invertible hash function and an invertible hash function  
12 complement to at least the first resultant to provide the hash, the complement of the hash  
13 including the plurality of resultants except the first resultant.

1           2.       The method of claim 1 wherein the invertible hash function is an invertible  
2 geometric hash function and the invertible hash function complement an invertible  
3 geometric hash function complement.

1           3.       The method of claim 1 wherein each of the plurality of components includes  
2 thirty-two bits.

1           4.       The method of claim 1 wherein the final component includes a plurality of  
2 bits used to pad the final component to the particular number of bits.

1           5.       The method of claim 1 wherein the invertible hash function and the invertible  
2 hash function complement providing step (c) further includes the step of:

3           (c1)     applying the invertible hash function and the invertible hash function  
4 complement to each of the plurality of resultants, the hash including the invertible hash  
5 function and the invertible hash function complement of the first resultant, the complement  
6 of the hash including the invertible hash function and the invertible hash function  
7 complement of each of the plurality of resultants except the first resultant.

1           6.       The method of claim 1 further comprising the step of:

2           (d)     providing a permutation of at least one component of the plurality of  
3 components.

1           7.       A method for providing a hash and a complement of the hash for an item in a  
2 computer system, the method comprising the steps of:

3           (a)     providing a plurality of components from the item, the plurality of  
4 components including a first component and a last component, each of the plurality of  
5 components includes a particular number of bits;

6           (b)     applying an invertible hash function and an invertible hash function  
7 complement to at least the first component of the plurality of components;

8           (c)     cascading the plurality of components through at least one XOR to provide a

9 plurality of resultants, the plurality of resultants including a first resultant and a final  
10 resultant, the final resultant including only the last component and the first resultant  
11 including an XOR of the first component and remaining cascaded components of the  
12 plurality of components, the hash including the first resultant and the complement of the  
13 hash including the plurality of resultants except the first resultant.

1 8. The method of claim 7 wherein the invertible hash function is an invertible  
2 geometric hash function and the invertible hash function complement is an invertible  
3 geometric hash function complement.

1 9. The method of claim 7 wherein each of the plurality of components includes  
2 thirty-two bits.

1 10. The method of claim 7 wherein the final component includes a plurality of  
2 bits used to pad the final component to the particular number of bits.

1 11. The method of claim 7 wherein the invertible hash function and the invertible  
2 hash function complement providing step (b) further includes the step of:

3 (b1) applying the invertible hash function and the invertible hash function  
4 complement to each of the plurality of components.

1 12. The method of claim 7 further comprising the step of:

2 (d) providing a permutation of at least one component of the plurality of

components.

13. A computer-readable medium containing a program for providing a hash and a complement of the hash for an item in a computer system, the program including instructions for:

(a) providing a plurality of components from the item, the plurality of components including a first component and a last component, each of the plurality of components includes a particular number of bits;

(b) cascading the plurality of components through at least one XOR to provide a plurality of resultants, the plurality of resultants including a first resultant and a final resultant, the final resultant including only the last component and the first resultant including an XOR of the first component and remaining cascaded components of the plurality of components; and

(c) applying an invertible hash function and an invertible hash function complement to at least the first resultant to provide the hash, the complement of the hash including the plurality of resultants except the first resultant.

14. The computer-readable medium of claim 13 wherein the invertible hash function is an invertible geometric hash function and the invertible hash function complement is an invertible geometric hash function complement.

15. The computer-readable medium of claim 13 wherein each of the plurality of components includes thirty-two bits.

1           16.    The computer-readable medium of claim 13 wherein the final component  
2 includes a plurality of bits used to pad the final component to the particular number of bits.

1           17.    The computer-readable medium of claim 13 wherein the invertible hash  
2 function and the invertible hash function complement providing instructions (c) further  
3 includes instructions for:

4           (c1)   applying the invertible hash and the invertible hash function complement to  
5 each of the plurality of resultants, the hash including the invertible hash function and the  
6 invertible hash function complement of the first resultant, the complement of the hash  
7 including the invertible hash function and the invertible hash function complement of each  
8 of the plurality of resultants except the first resultant.

1           18.    The computer-readable medium of claim 13 further comprising instructions  
2 for:

3           (d)    providing a permutation of at least one component of the plurality of  
4 components.

1           19.    A computer-readable medium for providing a hash and a complement of the  
2 hash for an item in a computer system, the program including instructions for:

3           (a)    providing a plurality of components from the item, the plurality of  
4 components including a first component and a last component, each of the plurality of  
5 components includes a particular number of bits;

6           (b)    applying an invertible hash function and an invertible hash function

7 complement to at least the first component of the plurality of components;

8 (c) cascading the plurality of components through at least one XOR to provide a  
9 plurality of resultants, the plurality of resultants including a first resultant and a final  
10 resultant, the final resultant including only the last component and the first resultant  
11 including an XOR of the first component and remaining cascaded components of the  
12 plurality of components, the hash including the first resultant and the complement of the  
13 hash including the plurality of resultants except the first resultant.

1 20. The computer-readable medium of claim 19 wherein the invertible hash  
2 function is an invertible geometric hash function and the invertible hash function  
3 complement is an invertible geometric hash function complement.

1 21. The computer-readable medium of claim 19 wherein each of the plurality of  
2 components includes thirty-two bits.

1 22. The computer-readable medium of claim 19 wherein the final component  
2 includes a plurality of bits used to pad the final component to the particular number of bits.

1 23. The computer-readable medium of claim 19 wherein the invertible hash  
2 function and the invertible hash function complement providing instructions (b) further  
3 includes instructions for:

4 (b1) applying the invertible hash function and the invertible hash function  
5 complement to each of the plurality of components.

1           24.    The computer-readable medium of claim 19 further comprising instructions  
2 for:

3           (e)    providing a permutation of at least one component of the plurality of  
4 components.

1           25.    A system for providing a hash and a complement of the hash for an item in a  
2 computer system, the system comprising:

3           means for providing a plurality of components from the item, the plurality of  
4 components including a first component and a last component, each of the plurality of  
5 components includes a particular number of bits;

6           means for cascading the plurality of components through at least one XOR to provide  
7 a plurality of resultants, the plurality of resultants including a first resultant and a final  
8 resultant, the final resultant including only the last component and the first resultant  
9 including an XOR of the first component and remaining cascaded components of the  
10 plurality of components; and

11          means for applying an invertible hash function and an invertible hash function  
12 complement to at least the first resultant to provide the hash, the complement of the hash  
13 including the plurality of resultants except the first resultant.

1           26.    The system of claim 25 wherein the invertible hash function is an invertible  
2 geometric hash function and the invertible hash function complement is an invertible  
3 geometric hash function complement.

1           27.     The system of claim 25 wherein each of the plurality of components includes  
2 thirty-two bits.

1           28.     The system of claim 25 wherein the final component includes a plurality of  
2 bits used to pad the final component to the particular number of bits.

1           29.     The system of claim 25 wherein the invertible hash function providing means  
2 further includes:

3                 means for applying the invertible hash function and the invertible hash function  
4 complement to each of the plurality of resultants, the hash including the invertible hash  
5 function and the invertible hash function complement of the first resultant, the complement  
6 hash including the invertible hash and the invertible hash function complement of each of  
7 the plurality of resultants except the first resultant.

1           30.     The system of claim 25 further comprising:  
2                 means for providing a permutation of at least one component of the plurality of  
3 components.

1           31.     A system for providing a hash and a complement of the hash for an item in a  
2 computer system, the system comprising:

3                 means for providing a plurality of components from the item, the plurality of  
4 components including a first component and a last component, each of the plurality of  
5 components includes a particular number of bits;

6 means for applying an invertible hash function and an invertible hash function  
7 complement to at least the first component of the plurality of components; and

8 means for cascading the plurality of components through at least one XOR to provide  
9 a plurality of resultants, the plurality of resultants including a first resultant and a final  
10 resultant, the final resultant including only the last component and the first resultant  
11 including an XOR of the first component and remaining cascaded components of the  
12 plurality of components, the hash including the first resultant and the complement of the  
13 hash including the plurality of resultants except the first resultant.

1 32. The system of claim 31 wherein the invertible hash function is an invertible  
2 geometric hash function and the invertible hash function complement is an invertible  
3 geometric hash function complement.

1 33. The system of claim 31 wherein each of the plurality of components includes  
2 thirty-two bits.

1 34. The system of claim 31 wherein the final component includes a plurality of  
2 bits used to pad the final component to the particular number of bits.

1 35. The system of claim 31 wherein the invertible hash function and the  
2 invertible hash function complement providing means further includes:

3 means for applying the invertible hash function and the invertible hash function  
4 complement to each of the plurality of components.

1           36.     The system of claim 31 further comprising:

2               means for providing a permutation of at least one component of the plurality of

3     components.

CONFIDENTIAL